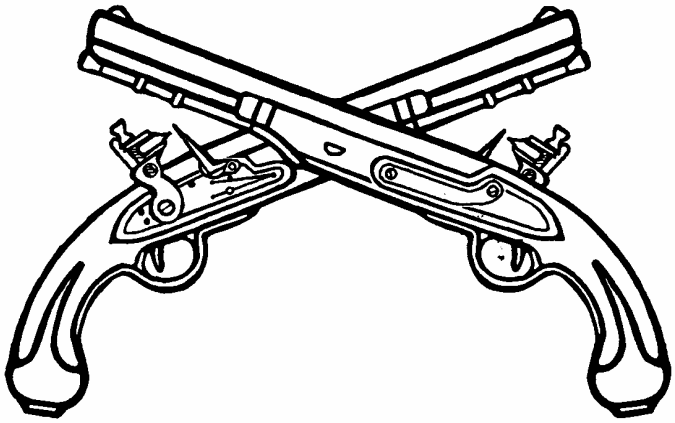
SUBCOURSE
MP1000

EDITION
C

PHYSICAL SECURITY PLANNING

MP



SETS THE STANDARD FOR EXCELLENCE

THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT

ARMY CORRESPONDENCE COURSE PROGRAM

A I P D

READINESS / PROFESSIONALISM



THRU GROWTH

PHYSICAL SECURITY PLANNING

Subcourse Number MP1000

EDITION C

United States Army Military Police School
Fort McClellan, Alabama 36205-5030

5 Credit Hours

Edition Date: March 1996

SUBCOURSE OVERVIEW

We designed this subcourse to teach you to perform duties as a physical security specialist/supervisor and it covers information ranging from basic physical security measures to development of a complete physical security plan.

There are no prerequisites for this subcourse.

This subcourse reflects the doctrine which was current at the time it was prepared. In your own work situation, always refer to the latest official publications.

Unless otherwise stated, the masculine gender of singular pronouns is used to refer to both men and women.

TERMINAL LEARNING OBJECTIVE

ACTION: You will identify the duties of a physical security specialist in reviewing physical security plans, conducting physical security inspections and surveys, organizing a physical security education program, and supervise security force operations.

CONDITION: You will have this subcourse, paper and pencil.

STANDARD: To demonstrate competency of this task you will have to achieve a minimum score of 70 percent on the final subcourse examination.

TABLE OF CONTENTS

Section Page

Subcourse Overview.....i

Administrative Instructions.....iii

Grading and Certification Instruction.....iii

Lesson 1: Review a Physical Security Plan.....1-1

Practice Exercise.....1-11

Answer Key and Feedback.....1-12

Lesson 2: Conduct Physical Security Inspection and Surveys 2-1

Practice Exercise.....2-13

Answer Key and Feedback.....2-16

Lesson 3: Organize a Physical Security Education Program.....3-1

Practice Exercise.....3-6

Answer Key and Feedback.....3-8

Lesson 4: Supervise Security Force Operations.....4-1

Part A: Security Force Mission and Function.....4-1

Part B: Security Supervisor 4-8

Part C: Training 4-11

Practice Exercise.....4-19

Answer Key and Feedback.....4-22

Examination.....E-1

Student Inquiries

THIS PAGE INTENTIONALLY LEFT BLANK

LESSON 1

REVIEW A PHYSICAL SECURITY PLAN

Critical Task: 191-386-0002

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn the components of a physical security plan and how to write one.

TERMINAL LEARNING OBJECTIVE:

ACTION: Write a physical security plan.

CONDITION: You will have this subcourse, paper and pencil.

STANDARD: To demonstrate competency of this task you must achieve a minimum score of 70 percent on the final subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications: AR 190-13 and FM 3-19.30.

INTRODUCTION

All commanders must ensure that certain reasonable safeguards are taken. They must protect personnel, property, and operations under their command against any threats. Responsibility is normally assigned to the provost marshal or physical security officer. Each security officer faces problems peculiar to his post; thus, each must develop a detailed written plan. The plan will use resources in the best way to provide enough security. Security planning entails a cooperative systematic approach. This includes agents from tenant activities on the post. This approach also includes use of Army regulations and MP doctrine. All are necessary for an effective physical security plan.

1. Definition of Physical Security Plan. A comprehensive written plan providing proper and economical use of personnel and equipment to prevent or minimize loss or damage from theft, misuse, espionage, sabotage, and other criminal or disruptive activities.

2. Purpose of Physical Security Plan. The purpose of a physical security plan is threefold. It should provide guidance, assign responsibility, and it should also set minimum standards for the security of property and personnel.

3. Planning Considerations. The physical security officer must first determine the types and extent of protection required on a post. He must do so by considering certain pertinent factors in their respective order.

a. Mission. Mission importance to the Army's and post's continuing mission must be determined.

b. Threats. Installations will develop a local threat statement to identify local activities that threaten Army property and personnel in the geographical area.

c. Area. Analysis of area to be protected must be considered. Such analysis would include the nature and arrangement of activity. It would also include number of personnel involved. Monetary, tactical or strategic value of material, storage of classified information and equipment. As a process of area analysis, installation commanders will designate, in writing, mission essential or vulnerable areas (MEVAs) under their control. Also, risk analysis will be performed in accordance with AR 190-51 for all facilities designated or likely to be designated as MEVAs.

d. Criticality and vulnerability. Threats to information, equipment, or material must be known and analyzed.

e. Operation, maintenance, and other requirements. All these must be woven into the plan to avoid mission interruption.

f. Environment. Political, economic, and legal factors are important. So are the terrain, weather, and climate.

g. Cost of material and equipment, and available funds. Available resources determine the possible degree of protection.

h. Changes in operation. Possible expansion, relocation, and other changes must be considered.

i. Cost effective protection. The best method of providing cost effective protection for personnel and equipment must be determined.

4. Physical Security Plan.

a. A physical security plan will include the following:

(1) Purpose. This would include scope, use, and applicability. It would also include any special contingencies.

(2) Area security. Definition and designation of areas that are considered critical would be included. Establishment of priorities must be set for the protection of these areas.

(3) Control measures. These would include restrictions on access and movement into security areas. For example, restrictions would need to be on

personnel identification and movement control. Control would be needed over vehicles and materials.

(4) Aids to security. Such aids would include perimeter barriers and protective alarm. Lighting and communications systems would also aid.

(5) Security force operations. Detailed special orders/SOPs will be attached as annexes.

(6) Contingency plans. Detailed plans for disaster, of fire, etc., will be attached as annexes.

(7) Use of air surveillance.

(8) Coordinating instructions. Such instructions would include coordination of intelligence and physical security roles. Coordination with all interested staff members must be spelled out. Coordination will integrate the plan and its measures with other security operational functions; it will make the plan work. Lack of such integration will result in waste of money, equipment, and manpower. More importantly, the lack can endanger the security of a post.

b. The physical security plan that follows is a sample of one adapted from FM 3-19.30. Carefully study the outline. Knowing the minimum requirements for a security plan adds much to an organized effective program. Other lessons expand on areas covered by this plan. The total provides a complete view of physical security.

SAMPLE
PHYSICAL SECURITY PLAN

(Classification)

Copy No.
Issuing
Headquarters
Place of issue
Date of issue

PHYSICAL SECURITY PLAN

1. Purpose. State purpose of the plan.

2. Area Security. Define the areas, buildings, and other structures considered critical; establish priorities for their protection.

3. Control Measures. Define and establish restrictions on access and movement into critical areas. These restrictions can be categorized. Categories would include personnel, vehicles, and materials.

a. Personnel Access:

(1) Establish controls pertinent to each area or structure.

(a) Authority for access.

(b) Access criteria for:

1 Unit personnel.

2 Visitors.

3 Maintenance personnel.

4 Contractor personnel.

5 National Guard.

(2) Identification and control.

(a) Describe the system to be used in each area. A badge system may be used. If so, complete description of all aspects being used. This description would include distribution requirements for identification and control of personnel doing business on the post.

(Classification)

(b) Application of the system.

1 Unit personnel.

2 Visitors to restricted areas.

3 Visitors to administrative areas.

4 Vendors, tradesmen, etc.

5 Contractor personnel.

6 Maintenance or support personnel.

b. Material Control.

(1) Incoming.

(a) Requirements for admission of material and supplies.

(b) Search and inspection of material for possible sabotage hazards.

(c) Special controls on delivery of supplies and/or personnel shipments in restricted areas.

(2) Outgoing.

(a) Documentation required.

(b) Controls, as outlined in (l)(a), (b), and (c) above.

(c) Classified shipments NOT involving nuclear/chemical material.

(3) Nuclear/chemical material.

(a) Controls on movement of warheads/chemicals on the installation.

(b) Controls on shipments or movement of training warheads/chemicals.

(c) Controls on pickup or delivery of warheads/chemicals outside the installation.

c. Vehicle Control.

(1) Policy on search of military and privately owned vehicles.

(2) Parking regulations.

(3) Controls for entrance into restricted and administrative areas.

(a) Privately owned vehicles.

(b) Military vehicles.

(c) Emergency vehicles.

d. Vehicle Registration.

4. Aids to Security. Indicate how the following listed aids to security will be implemented on post.

a. Protective barriers.

(1) Definition.

(2) Clear zones.

(a) Criteria.

(b) Maintenance.

(3) Signs.

(a) Types.

(b) Posting.

(4) Gates.

(a) Hours of operation.

(b) Security requirements.

(c) Lock security.

b. Protective lighting system.

(1) Use and control.

(2) Inspection.

(3) Action to be taken in the event of commercial power failure.

(4) Action to be taken in the event of a failure of alternate source of power.

(5) Emergency lighting systems.

(a) Stationary.

(b) Portable.

c. Intrusion Detection Systems.

(1) Security classifications.

(2) Inspection.

(3) Use and monitoring.

(4) Action to be taken in event of "alarm" conditions.

(5) Maintenance.

(6) Alarm logs or registers.

(7) Sensitivity settings.

(8) Fail-safe and tamper-proof provisions.

(9) Monitor panel location.

d. Communications.

(1) Locations.

(2) Use.

(3) Test.

(4) Authentication.

5. Security Forces. Include general instructions that would apply to all security force personnel (fixed and mobile). Detailed instructions, such as Special Orders and SOP should be attached as annexes.

a. Composition and organization.

b. Tour of duty.

c. Essential posts and routes.

d. Weapons and equipment.

e. Training.

f. Use of sentry/patrol dogs.

g. Method of challenging with sign and countersign.

h. Alert force.

(1) Composition.

(2) Mission.

(3) Weapons and equipment.

(4) Location.

(5) Deployment concept.

6. Contingency Plans. Indicate required actions in response to various emergency situations. Detailed plans such as counterterrorism, bomb threats, hostage negotiation, disaster, fire, etc., should be attached as annexes.

a. Individual actions.

b. Alert force actions.

c. Security force actions.

7. Use of Air Surveillance.

8. Coordinating Instructions. Indicate matters which require coordination with other military and civil agencies.

a. Integration with plans of host or nearby military installations.

b. Liaison and coordination.

(1) Local civil authorities.

(2) Federal agencies.

(3) Military organizations.

/s/_____
Commander

Annexes:

A - Intelligence

B - Installation Security Status Map

C - Contingency Plans

D - Special Instructions to Security Officers/Managers and Officers of the Day

E - Commander of Relief Instructions

F - Sergeant of the Guard Instructions

G - Special Orders for Guard Posts

THIS PAGE WAS LEFT BLANK INTENTIONALLY

LESSON 1

PRACTICE EXERCISE

REQUIREMENT. The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. You are assigned as the post physical security officer. What is your primary concern in developing a physical security plan?

A. Political environment.
B. Criticality.
C. Mission.
D. Changes in operation.

2. Which of the following IS NOT classified as a security aid?

A. Protective barriers.
B. Lighting systems.
C. Personnel control.
D. Communication system.

3. Your contingency physical security plan indicates which of the following?

A. Fail-safe and tamper-proof provisions.
B. Required actions in response to various emergency situations.
C. Procedures for coordinating with only local civil authorities.
D. Requirements for conducting a security survey.

LESSON 1

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	C.	Mission Mission. Mission... (page 1-2, para 3a)
2.	C.	Personnel control Aids to security... (page 1-3, para 4a(4))
3.	B.	Required actions in response to various emergency situations Contingency plans of... (page 1-3, para 4a(6))

LESSON 2

CONDUCT PHYSICAL SECURITY INSPECTIONS AND SURVEYS

Critical Task: 191-386-0024

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn the fundamental principles in the use of inspections and surveys.

TERMINAL LEARNING OBJECTIVE:

ACTION: Identify the fundamental principles in the use of inspections and surveys.

CONDITION: You will have this subcourse, pencil and paper.

STANDARD: To demonstrate competency of this task you must achieve a minimum score of 70 percent on the final subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publications: AR 190-13, AR 190-51, and FM 3-19.30.

INTRODUCTION

Physical security programs are a part of the Army Force Protection Plan. As such, they must present broad measures meant to safeguard personnel. Such programs must prevent illegal access to equipment, buildings, materiel, and papers. These must be safeguarded against espionage, sabotage, damage, and theft. A physical security program must contain measures for such safety. At the least, these programs will include the physical security plan. Programs will also include physical security inspections and surveys. Lastly, such programs will include an ongoing assessment of the post's physical security stance.

1. Physical Security.

a. Detection, prevention, and protection are the main concerns of these programs. Physical security is that part meant to safeguard personnel, property, and operations. It prevents illegal access to equipment, buildings, materiel, and papers. These aforementioned are thus protected against espionage. They are safeguarded also from sabotage, damage, and theft. Physical security is an important part of the crime prevention program.

b. For greatest efficiency, all security measures should complement and supplement each other. Coordinating security measures with other activities eliminates duplication of effort. It eliminates waste of resources, also, and ensures a sound, effective program.

2. Responsibilities.

a. Defined levels of responsibilities can aid the success of any operation. It promotes cooperation in any activity having dual responsibility for a task. No two physical security plans should be the same, however. It is important, therefore, that staff and command relationships related to physical security are defined. Such action will provide procedure and guidance for all activities.

b. Headquarters, Department of the Army, channels responsibilities in physical security through local command levels.

(1) Law Enforcement Division, Deputy Chief of Staff for Operations (DCSSOPS). This division provides Armywide policies and procedures regarding physical security. They also provide guidance and assistance in this regard.

(2) Assistant Chief of Staff of Intelligence. This office is responsible for counterintelligence in respect to protection. They safeguard the Army from espionage, sabotage, and subversion.

(3) Local commanders. They ensure that reasonable precautions are taken to safeguard personnel and property in their command.

(a) Physical Security Officers. Designated by commanders, they are responsible for planning and coordinating physical security matters.

(b) Physical Security Inspectors. These persons are certified by their local command. They are graduates of the U.S. Army Military Police School (USAMPS) Physical Security Course.

3. Physical Security Inspection. This inspection is a formal one. It is a recorded assessment of physical security measures. Such measures are designed for mission essential or vulnerable areas.

a. A physical security inspection is designed for specific individual activities. These are activities wherein one or more threats may easily cause loss, damage, or destruction. Such events would affect the mission of the whole post. This inspection assists the command in evaluating the adequacy of existing physical security safeguards.

b. The following may be considered critical and vulnerable facilities:

(1) Ammunition storage point.

(2) Command post (main and alternate).

(3) Consolidated weapons storage facilities.

(4) Finance offices.

(5) Motor pool.

(6) Intrusion detection system monitor stations.

(7) Petroleum, oils, and lubricants (POL) storage and dispensing points.

(8) Water sources.

(9) Medical supply storage facilities.

(10) Communications center.

c. Some activities on a post may be exempt from inspections. Exemption may be due to their specific missions. These activities may be inspected under guidance and directive unique to their missions.

d. The physical security officer must coordinate with COs of exempt activities. They must do so to verify exemption status.

e. A physical security inspection is done to verify current data and obtain new facts. It should provide data for a true assessment of existing threats. The inspection should also determine the effectiveness of current safety measures.

f. An inspection team is useful. It permits members to develop expertise in inspecting certain aspects of physical security. For example, one member may look at the use and training of security guards, another may inspect the perimeter barriers and protective lighting system. This division of duties allows for a more complete inspection and assessment.

4. Relationship to Physical Security Surveys. Physical security inspections of mission essential and vulnerable areas are necessary. However, they do not replace requirements for surveys. Inspections provide a large part of the data base for the annual/biannual physical security survey.

a. A physical security survey includes in its scope an entire post. The survey includes all of the activities and facilities of that post.

b. A physical security inspection is limited. It covers only specific individual activities at a post or facility.

c. Inspections supplement surveys. They do so by providing a more detailed, closer examination of specific activities. Inspections also provide important data as a supplement to the surveys.

5. Relationship to Crime Surveys. A crime survey is a formal review or study of conditions within a facility, activity, or area. Its purpose is threefold:

(1) for discovering crime; (2) for evaluating the opportunity for criminal acts; and (3) for identifying conditions conductive to criminal acts. Crime surveys are performed by U.S. Army Criminal Investigation Command (USACIDC) special agents. These crime surveys serve to help the post crime prevention programs in many ways. Crime surveys do not replace physical security inspections or physical security surveys. They are not routinely scheduled like physical security or crime prevention inspections, but are requested. Crime surveys are performed when competent authority determines that a need has been created by factors beyond his control. The requester may be any CO, supervisor of USACIDC, or field office commander. Examples of factors beyond control may be: unexplained losses or shortages, changes in the local political environment, or a series of unsolved break-ins in the areas. Crime survey reports, if available, should be reviewed prior to the beginning of physical security inspections or surveys of the same area.

6. Inspection Personnel. Installation physical security inspectors will be selected by the provost marshal (PM), security officer, or Commander, Law Enforcement Activity (LEA).

a. Standards for selecting physical security inspectors.

(1) Qualified in the primary MOS 95B or 95C.

(2) SSG or above (may be waived to SGT).

(3) Successful completion of the Conventional Physical Security Course (7H-31D/830-ASI H-3) conducted by USAMPS.

(4) Cleared for access to secret national defense information.

(5) Cleared by a favorable crime records center (CRC) name check.

b. Standards for obtaining physical security inspector credentials are as follows:

(1) The only authorized credentials for physical security inspectors are DA Form 4261 and DA Form 4261-1 (Physical Security Inspector Identification Card)(see Figure 2-1).

(2) DA Form 4261 will be authenticated by the PM, security officer, or commander, USDB.

(3) Inspector credentials will not be issued without a favorable CRC name check.

7. Type of Inspection or Survey.

a. Preoccupancy inspection. A new or renovated building is often the locale of a mission essential activity. If so, a security inspection of the

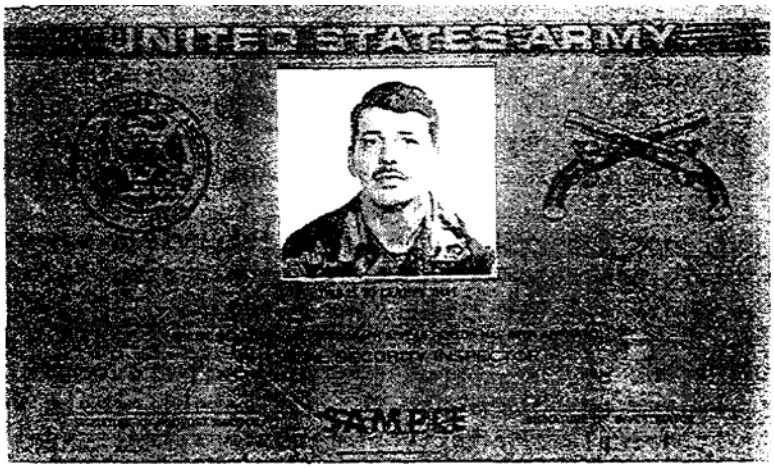
area should be done to detect any structural deficiencies. Such inspection must occur before the government signs over the buildings from a contractor.

b. Initial inspection or survey. This is the first physical security inspection on record. Such is the case regardless of the form used or when the first Inspection is done. The first inspection occurs when a mission essential or vulnerable area is selected for use.

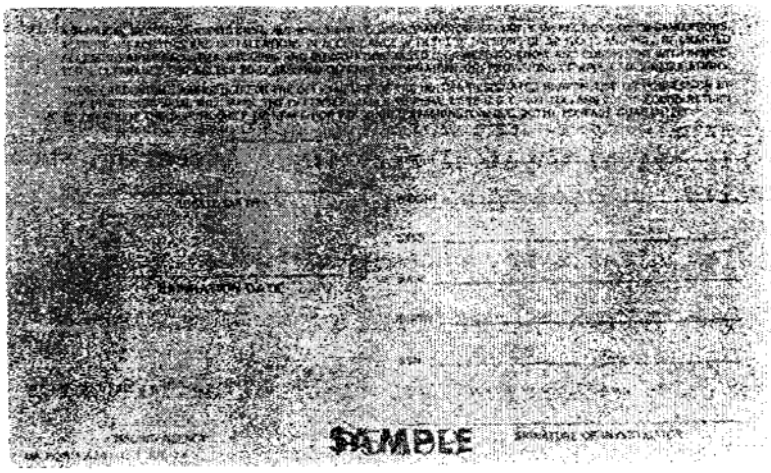
c. Recurring Survey/Inspection.

(1) Inspections will be conducted every 18 months for nuclear reactors and nuclear/chemical storage units/activities, conventional arms and ammunition storage units, and critically sensitive ADP activities or facilities.

(2) Every two years for other mission essential or vulnerable areas or activities as directed by the local commander.



DA Form 4261



DA Form 4261

Figure 2-1. Physical Security Inspector Credentials.

(3) Surveys will be conducted every three years except for those installations with the mission of nuclear, chemical, or conventional arms and ammunition storage. These installations will be surveyed every 18 months.

(4) Critically sensitive, highly sensitive, sensitive, and nonsensitive ADP activities or facilities will be surveyed every 24 months.

8. Methods of Inspection. There are two types of inspection methods: announced and unannounced.

a. Announced inspection. Commanders are informed of the inspection. Therefore, they have a chance to upgrade their areas' security.

b. Unannounced inspection. Commanders are not informed of the inspection. This gives the inspector a picture of the day-to-day operation of the area, which could identify weaknesses in the security of a building.

9. Inspection Aids. Performing an inspection requires careful planning. Know what aids are available and how they may aid your inspection. Some aids include: FMs 3-19.30 and 19-10, ARs 190-11, 190-13, and 190-51. Remember, regulations change, so you must be alert to changes affecting physical security. Crime prevention inspection reports, crime surveys, safety or fire reports, and floor plans or blueprints should not be overlooked.

10. Inspection Entrance Interview. Entrance interviews are required prior to conducting the actual inspection with the CO or his agent. The interview is the first of three phases of the inspection process. Team members are introduced; mission and procedures are explained. Assistance is requested, the need for cooperation by the inspection team and the commander is stressed. There are two advantages to this approach: it establishes a working relationship, and it downplays negative impressions that usually accompany inspection teams. Your purpose is to assist the commander by identifying physical security weaknesses and by recommending corrective action.

11. Inspection Procedures. The inspection is the second phase of the three-phase inspection.

a. All data pertaining to the activity must be reviewed. Data includes both current and historical physical security. Attention should be given to the following details:

(1) Security directives, plans, and SOPs.

(2) Previous inspection reports.

(3) Valid work orders for correction of deficiencies.

(4) Waivers and exceptions.

(5) Reply by endorsements (RBIs) from previous inspections.

(6) Past security related incidents.

b. One of the most important guides for an inspector is a comprehensive inspection checklist. Appendix O, FM 3-19.30, gives good examples of physical security checklists. However, security personnel should be alert. They must avoid sole reliance on the checklist. There will be areas of security importance not listed. These areas must also be reviewed. Unit commanders and first sergeants must be informed that although you may use a checklist, other areas may also be inspected. This should be printed on the checklist, so there will be no confusion. There is no set format for a checklist; the one mentioned may be used as a basis for a locally produced report.

c. DA Form 2806-1-R (Physical Security Inspection Report) is used to record the physical security inspection (see figure 2-2).

d. DA Form 2806-R (Physical Security Survey Report) is used to record the physical security survey (see figures 2-3 and 2-4).

12. Standards of Security.

a. Certain standards should be used as a guide in judging a security program. These standards are dealt with in this lesson, FM 3-19.30, and other related security regulations. First consider the minimum standards of security. Then consider the facts brought out by the inspection. A careful balance must then be sought. Such balance should occur between what exists, what is desired, and what may be necessary due to national security. Certain deficiencies affect the entire post. These may be identified through physical security inspections. They include the following:

(1) Perimeter security is inadequate.

(2) There is evidence that a part of the post is being used for unlawful or unauthorized practices.

(3) Fences or lights are needed.

(4) Control and check of personnel entering or leaving the post are inadequate.

b. Inspection of facilities should include the following list of inquiries. However, inspections are not limited to these:

(1) Determine the steps being used for teaching persons the use of internal control procedures. Also, is there awareness of the need for alertness? Such awareness could prevent loss of money and property.

(2) Inquire into receiving, stock control, and storage procedures.

(3) Investigate steps used for receiving, holding, and banking money.

M TAB TAB TAB

PHYSICAL SECURITY INSPECTION REPORT

For use of this form, see AR 190-13; the proponent agency is DCSPER.

Requirement Control Symbol CSGPA-1671

1. REPORT NUMBER

2. DATE OF INSPECTION

3. PREPARING AGENCY

4. UNIT OR ACTIVITY INSPECTED

5. NAME AND RANK OF UNIT/ACTIVITY COMMANDER

6. REPORT NUMBER AND DATE OF PREVIOUS INSPECTION

7. UNIT OR ACTIVITY MISSION

8. TYPE OF AREA INSPECTED

9. TYPE INSPECTION

____ ANNOUNCED ____ UNANNOUNCED

10. HAS THE UNIT BEEN PROVIDED THE:

	YES	NO	NA
a. INSTALLATION PHYSICAL SECURITY THREAT STATEMENT?			
b. INSTALLATION PHYSICAL SECURITY PLAN?			

11. FINDINGS/RECOMMENDATIONS

12. INSPECTING OFFICIAL'S EVALUATION

13. RATING: THE SECURITY OF THIS UNIT/ACTIVITY IS:

____ ADEQUATE ____ NOT ADEQUATE

TO PROTECT THE ARMY INTERESTS.

14. EXIT INTERVIEW *(Name, Grade or Rank, and Duty Position)*

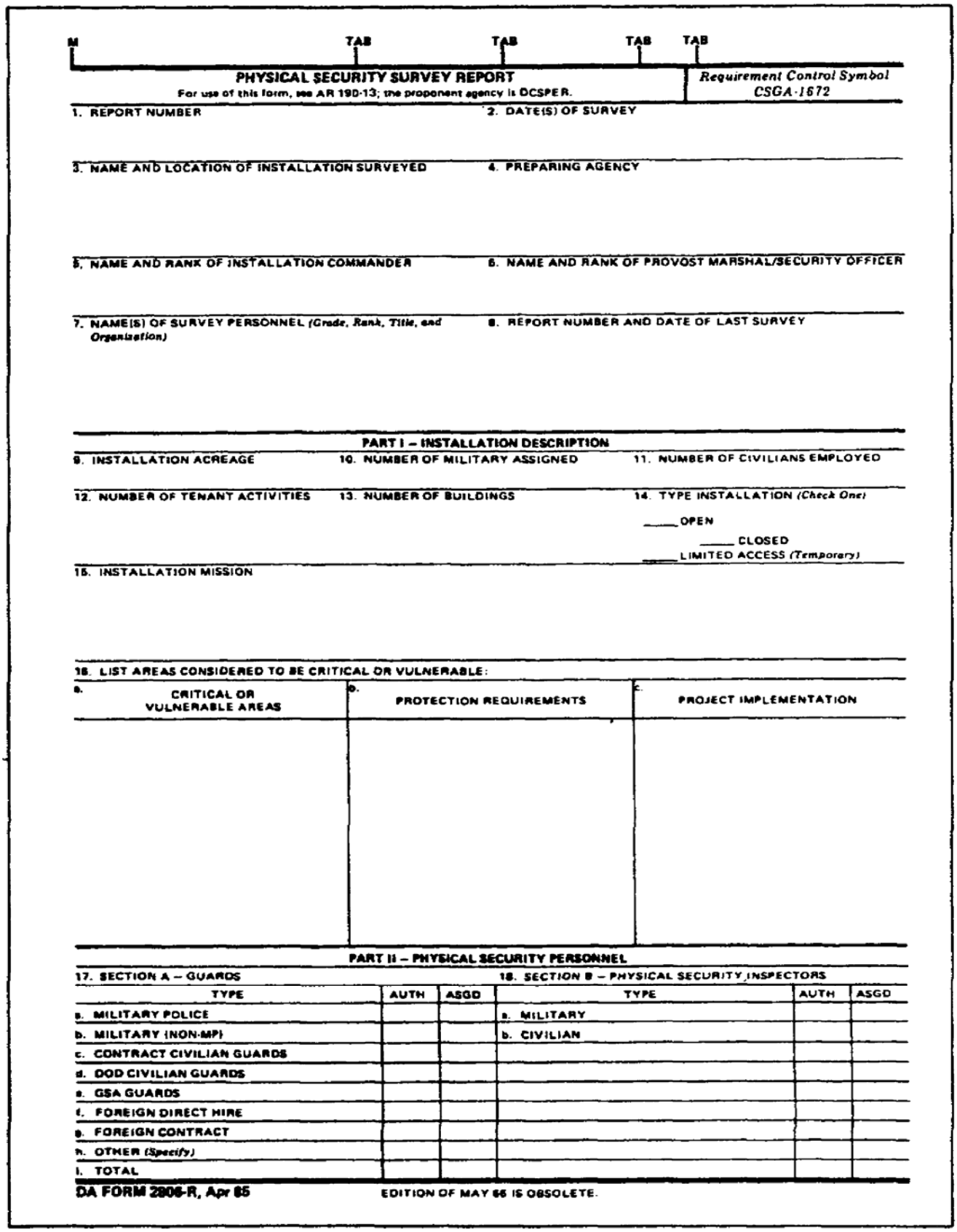
15a. INSPECTOR *(Name and Rank)* b. SIGNATURE c. DATE

16a. APPROVING AUTHORITY *(Name, Rank, Title)* b. SIGNATURE c. DATE

17. DISTRIBUTION:

DA FORM 2806-1-R, Apr 85

Figure 2-2. Physical Security Inspection Report, DA Form 2806-1-R.



M TAB TAB TAB TAB

PHYSICAL SECURITY SURVEY REPORT

For use of this form, see AR 190-13; the proponent agency is DCSPER.

Requirement Control Symbol CSGA-1672

1. REPORT NUMBER
2. DATE(S) OF SURVEY
3. NAME AND LOCATION OF INSTALLATION SURVEYED
4. PREPARING AGENCY
5. NAME AND RANK OF INSTALLATION COMMANDER
6. NAME AND RANK OF PROVOST MARSHAL/SECURITY OFFICER
7. NAME(S) OF SURVEY PERSONNEL *(Grade, Rank, Title, and Organization)*
8. REPORT NUMBER AND DATE OF LAST SURVEY

PART I – INSTALLATION DESCRIPTION

9. INSTALLATION ACREAGE
10. NUMBER OF MILITARY ASSIGNED
11. NUMBER OF CIVILIANS EMPLOYED
12. NUMBER OF TENANT ACTIVITIES
13. NUMBER OF BUILDINGS
14. TYPE INSTALLATION *(Check One)*
____ OPEN
____ CLOSED
____ LIMITED ACCESS *(Temporary)*
15. INSTALLATION MISSION
16. LIST AREAS CONSIDERED TO BE CRITICAL OR VULNERABLE:

a. CRITICAL OR VULNERABLE AREAS	b. PROTECTION REQUIREMENTS	c. PROJECT IMPLEMENTATION

PART II – PHYSICAL SECURITY PERSONNEL

17. SECTION A – GUARDS

TYPE	AUTH	ASGD
a. MILITARY POLICE		
b. MILITARY (NON-MP)		
c. CONTRACT CIVILIAN GUARDS		
d. DOD CIVILIAN GUARDS		
e. GSA GUARDS		
f. FOREIGN DIRECT HIRE		
g. FOREIGN CONTRACT		
h. OTHER *(Specify)*		
i. TOTAL		

18. SECTION B – PHYSICAL SECURITY INSPECTORS

TYPE	AUTH	ASGD
a. MILITARY		
b. CIVILIAN		

DA FORM 2806-R, Apr 65 EDITION OF MAY 65 IS OBSOLETE.

Figure 2-3. Physical Security Survey Report, DA Form 2806-R.

TAB TAB TAB

PART III – PHYSICAL SECURITY PLANNING

	YES	NO
19. HAS AN INSTALLATION PHYSICAL SECURITY THREAT STATEMENT BEEN PREPARED?		
20. HAVE SUBORDINATE UNITS OR TENANT ACTIVITIES BEEN PROVIDED A COPY?		
21. IS THERE AN INSTALLATION PHYSICAL SECURITY PLAN?		
a. DOES THE PLAN COVER PHYSICAL SECURITY FOR PEACETIME, MOBILIZATION, AND WARTIME?		
b. DOES THE PLAN INCLUDE ANNEXES FOR COUNTERTERRORISM, BOMB THREATS, ADP PLANS, AND WORK STOPPAGE PLANS AND INSTALLATION CLOSURE?		
22. DOES THE INSTALLATION PHYSICAL SECURITY PROGRAM SUPPORT OPERATIONS SECURITY AND CRIME PREVENTION PROGRAMS?		
23. IS PHYSICAL SECURITY INCLUDED IN INSTALLATION CONTINGENCY AND EXERCISE PLANS?		

24. BRIEFLY EXPLAIN "NO" ANSWERS OF ITEMS 19 THROUGH 23

25. FINDINGS/RECOMMENDATIONS

26. SURVEYING OFFICIAL'S EVALUATION

27. OVERALL EVALUATION OF PHYSICAL SECURITY PROGRAM

____EXCELLENT ____GOOD ____POOR

28a. SURVEY OFFICER *(Name, Grade, Organization)* b. SIGNATURE c. DATE

29a. APPROVING AUTHORITY *(Name, Rank, Title)* b. SIGNATURE d. DATE

30. DISTRIBUTION

31. DATE COMMANDER'S REPORT OF CORRECTIVE ACTION RECEIVED

Page 2, DA Form 2806-R, Apr 85

Figure 2-4. Physical Security Survey Report, DA Form 2806-R (Continued).

(4) Inspect the structural qualities of the buildings housing the facility.

(5) Determine the adequacy of security guards. Inquire about the effectiveness and enforcement of their orders.

(6) Establish current steps used for storing narcotics and sensitive medications. Find out how these drugs are accounted for.

c. Units on a post may also be inspected. Inspections may include the following list. However, inquiries are not limited to these:

(1) Determine the supply and storage room security procedures. Give special attention to the security of arms and ammunition (AR 190-11).

(2) Determine the unit guards. Include in the inquiry the adequacy and application of guard orders.

(3) Establish how nonappropriate fund money and property are safeguarded.

d. Inspections of units and facilities may point out weaknesses in their building securities. Weaknesses may be found in the following areas:

(1) Locking devices and key control.

(2) Pass system, if used.

(3) The adequacy of bars and/or protective screening. Such may be found over windows, skylights, and like openings.

(4) The potential for unlawful entry. Such entry may occur through attics, boiler rooms, or basements. Air vents and crawl spaces under buildings also afford the chance of unlawful entry.

(5) The need for, or adequacy of, existing intrusion detection systems.

(6) Improper storage.

(7) Lack of, or inadequacy of, inventories and audits.

(8) Lack of supervision or control in the unit or activity.

(9) Indications of changes or alterations in records.

(10) Surplus amounts of items on hand and their openness to unauthorized persons.

(11) The refusal or failure to spot-check employee work habits. The lack of internal control measures to assure honesty or to detect dishonesty.

(12) Compensatory measures utilized in areas where waivers have been granted.

13. Recommendations.

a. The inspector has identified security weaknesses or deficiencies. Now it is the duty of the inspector to recommend sound, feasible solutions. The aim is to correct these problems.

b. Recommendations must be consistent with:

(1) Installation mission.

(2) Threat to the installation.

(3) Urgency or recommendation and remedial action necessary.

(4) Budget limitations.

(5) Facilities, materials, and support available.

(6) Regulatory requirements.

14. Exit Interview.

a. An exit interview is the third phase of the inspection. It should be conducted as soon as possible after the inspection. The inspection's goal and objectives should be restated.

b. Findings of the inspection will be discussed.

c. A copy of the inspection report will be forwarded through command channels. It will be sent not later than 30 days following completion of the inspection.

LESSON 2

PRACTICE EXERCISE

REQUIREMENT: The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. A physical security plan is which of the following?

 A. The installation crime prevention program.
 B. A part of the physical security program.
 C. Optional to the commander.
 D. An informal security assessment.

2. You must hire additional physical security inspectors on your post. Which of the following is a criteria for selection?

 A. At least SSG/E6.
 B. U.S. citizen.
 C. Top Secret clearance.
 D. Three years law enforcement experience.

3. Of the following statements, which is most accurate regarding a physical security inspection?

 A. A physical security inspection replaces a physical security survey.
 B. A physical security inspection is designed for specific individual activities.
 C. All activities, regardless of their mission, will be inspected annually.
 D. A physical security inspection should be a "surprise inspection."

4. You are planning a section meeting. You decide that you will tell your people that physical security inspections do which of the following?

 A. Replace the physical security survey.
 B. Are necessary parts to physical security surveys.
 C. Are nonessential parts of a crime survey.
 D. Do not improve a post's security posture.

5. At the meeting, you will tell your people that the correct form to use for a physical security survey report is which of the following?

A. DA Form 2806-R.
B. DA Form 3964-R.
C. DD Form 1162-R.
D. DA Form 3975-R.

6. As a physical security inspector, you are planning to inspect the arms room of Company C, 548th Ordnance Battalion. Before the inspection, you should do what?

A. Conduct an entrance interview.
B. Obtain permission from the unit commander.
C. Inform the post G3 of the inspection date.
D. Submit an inspection schedule to the post GI.

7. Inspection of conventional arms and ammunition storage facilities must be done every _____?

A. 6 months.
B. 12 months.
C. 18 months.
D. 24 months.

8. You are conducting an inspection entrance interview. You inform the group that your duty is to do what?

A. Reduce cost of physical security programs.
B. Assist the commander by identifying physical security weaknesses and make recommendations to correct these problems.
C. Ensure that unit commanders do not exceed regulatory requirements.
D. Identify poor management practices in the area of physical security.

9. You realize the importance of physical security inspections and know that they do what?

A. Are seldom used as management tools.
B. Require very little coordination and planning.
C. Assist the commander in evaluating the adequacy of existing physical security safeguards.
D. Hamper the commander in planning for physical security surveys and crime surveys.

10. Of the following, which IS NOT a type of inspection?

A. Initial.
B. Recurring every 18 months.
C. Recurring every 12 months.
D. Preoccupancy.

11. Unannounced physical security inspections are conducted to allow for what?

A. For upgrading of the security area.
B. Inspectors to observe normal operation of the areas.
C. Identification of security violators.
D. Accurate evaluation on an initial inspection.

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	B.	A part of the physical security program At the least, these... (page 2-1, Introduction)
2.	A.	At least SSG/E6 SSG or above... (page 2-4, para 6a(2))
3.	B.	A physical security inspection is designed for specific A physical security inspection is... (page 2-2, para 3a)
4.	B.	Are necessary parts to physical security surveys Inspections provide a large part (page 2-3, para 4c)
5.	A.	DA Form 2806-R DA Form 2806-R... (page 2-7, para 11d)
6.	A.	Conduct an entrance interview Entrance interviews are... (page 2-6, para 10)
7.	C.	18 months Inspections will be... (page 2-5, para 7c(1))
8.	B.	Assist the commander by identifying physical security Your purpose is... (page 2-6, para 10)
9.	C.	Assist the commander in evaluation the adequacy Your purpose is... (page 2-6, para 10)
10.	C.	Recurring every 12 months. Type of inspection or survey. (page 2-4, para 7a, b, c)
11.	B.	Inspectors to observe normal operations... This gives the inspector... (page 2-6, para 8b)

LESSON 3

ORGANIZE A PHYSICAL SECURITY EDUCATION PROGRAM

Critical Task: 191-386-0016

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to organize a physical security education program.

TERMINAL LEARNING OBJECTIVE:

ACTION: Organize a physical security education program.

CONDITION: You will have this subcourse, paper and pencil.

STANDARD: To demonstrate competency of this task you must achieve a minimum score of 70 percent on the subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publication: FM 3-19.30.

INTRODUCTION

Any good security program should be aided by an effective education program. Security personnel cannot do their jobs alone. They must have the interest and support of everyone on the post. Such interest and support can be had only through education programs.

1. Program Considerations.

a. A sound education program must approach security from a total systems view. It must be concerned not only with physical security measures meant to prevent acts such as pilfering; it must be concerned with ongoing analysis of present safety measures. It must also be concerned with evaluation of practical security measures at a desired level. Lastly, it must involve an awareness of various security needs. Such needs would be those of an activity or post. These needs would be based on the post or activity mission.

b. It is important that the education program include all aspects of the crime prevention program. See ARs 190-33, 195-10; and FM 3-19.30.

c. Every soldier and DA civilian are involved in protection. Security education is an important part of your physical security program. Such education should aid in the overall mission.

d. Your education program should encourage prompt reporting of security breaches. It should also attempt to:

(1) Reduce security violations.

(2) Provide feedback to improve protective measures.

(3) Reduce vulnerabilities.

(4) Improve security awareness. This should assist in the reporting of threat information.

(5) Gain cooperation for security measures.

2. Program Formulation. Develop your plan at the post level. This will require actions by each of the major commands. Education programs should be based upon vulnerability and criticality. Also, statistical data of incidents and criminal information is important. Formulation of such programs must aid crime prevention. The programs should also aid military intelligence educational efforts.

3. Program Objectives.

a. The objectives of a security education program are simple in concept. The goal is to acquaint all persons with the reasons for security measures and to ensure their cooperation. Everyone (military and civilian) must be concerned with security. Even if they do not work with classified material or in a restricted area, they should be concerned. You must impress upon them that a locked gate or file cabinet is only a small part of the overall security plan. You must continually remind them of this.

b. An ongoing program must be taught to selected persons. These will be mainly supervisors and other key personnel. The program should cover needed and useful topics. This is necessary to develop a high degree of security awareness.

4. Educational Requirements. Security awareness is not an inherent state of mind; it must be taught. Many people are naive and trusting; they accept things at face value. These traits are desirable, but they are not favorable to security awareness. Structural and mechanical aids to security are not good without the active support of everyone. All persons must be made aware of the constant threat of breaches of security. They must always be aware of their duty to detect and combat such threats. An education program must be continuous and forceful. It must provide the constant awareness that good security demands.

5. Personal Presentations.

a. At commander's call, these presentations should be most effective.

b. Formal instructions should be given at the unit and activity level.

c. Technical advice may be presented by the provost marshal or security manager.

d. Security content is presented in accordance with the 190-series Army regulations.

6. Graphic Media Aids.

a. Posters are good; they may be large in size, brief, and to the point. They can impart their message at a glance. Posters should be displayed where the most people pass and/or meet in a crowd.

b. Placards are used where people are expected to loiter and have time to read. Bulletin boards, telephone booths, vending machines, and recreation areas are examples.

c. Leaflets are economical. They are usually pocket size for easy carrying. Distribution of leaflets is determined by the CO or activity chief.

7. Indoctrination. AR 380-5 requires the CO to establish security orientation. This regulation also requires education programs within his command. The CO is to ensure the following:

a. Each person is oriented. Each is kept proficient in the security measures which apply to him and his duties.

b. All personnel are aware of their security responsibilities.

c. All newly assigned personnel must be given an initial security orientation. Reading of regulations is not enough to ensure complete understanding. Initial instruction should consist of a general orientation on the need for and dangers to security. Instruction should also stress the person's responsibility in preventing violations. It should include a discussion of those threats common to everyone. Emphasis should be placed on the dangers of loose talk and operational carelessness. It should define general security measures in effect. Examples might include the pass system, private vehicle control, and package inspection. Further instructions should be annotated on the person's duty assignment.

d. Further orientation should continue on an annual basis. Such orientation is prescribed by AR 381-12. This deals with Subversion and Espionage Directed Against the U.S. Army and Deliberate Security Violations.

e. AR 360-81 covers The Command Information Program. This discusses news media that can be used in security education programs. Included are those prescribed by AR 381-12.

8. Crime Prevention.

a. Security education programs should include material on the crime prevention programs. See AR 195-10, FM 19-10, and FM 19-20. Crime prevention programs should be those which are designed to reduce crime. Reduction is done by eliminating or reducing factors that cause criminal acts. Crime normally has three elements in common. These elements are ability, desire, and opportunity. An effective security education program will remove or lessen the chances of criminal acts.

b. FM 19-10 (Military Police Operations) provides guidance on leading a crime prevention program. Such a program includes both crime prevention surveys and education programs. The goals of the former were stated in the above paragraph. An education program emphasizes security awareness for everyone. It further teaches them the importance of securing and protecting military and personal property.

c. A security education program, then, provides an excellent means of passing out crime prevention information. The program urges everyone to participate. They can observe and report security deficiencies, violations, or hazards of any sort.

9. Program of Instruction.

a. The security manager is responsible for planning an effective program of instruction. Profitable use must be made of the limited time normally available for such instruction. Therefore, the techniques of a competent instructor are called for. The security manager should present the more important blocks of instruction; other competent instructors may present the less important. This depends on their areas of responsibility, training, and experience.

b. The offices listed below can aid the development of the program. These provide materials applicable to their areas of responsibility. Each can give additional aid by holding security briefings related to their areas.

Staff judge advocate
Chaplain
Special services officer
Safety director
Information officer
Post surgeon
CID representative
Character guidance council representative
Major organizational command representatives
Local police and allied agencies

c. Base the program on the total security posture of the post. It should begin with an explanation of the program, its aims, and objectives--the WHY.

d. Then, develop the necessary tools to reach those goals and objectives--the WHAT.

e. Describe the methods of education of the program. Do so through individual and group conferences, meetings, and speeches. Use the news media, posters, placards, leaflets, etc.--the HOW.

f. Provide for initial and refresher training. Also, provide for debriefing of appropriate persons. This will be needed upon their reassignment, retirement, departure on leave, and at other times.

g. Stress the absolute requirement for the support of every person. Do so regardless of the security clearance he may or may not have. Do so regardless of his work assignment.

h. As a minimum, include material on any recent incidents of security deficiency or violation. Also include material on any areas of laxity. If there are any trends in the security posture of the post, include this data also.

10. Scheduling and Testing.

a. Frequent, short periods of instruction are better than less frequent long periods. The ideas contained in four well-planned weekly 15-minute classes are more readily absorbed. Those contained in a 1-hour lecture once a month are not. This is so regardless of how well the latter is planned and delivered. Instruction that trespasses on the free time of the audience is seldom well received. Short periods to selected groups are easier to schedule without disrupting the operation.

b. In any form of instruction, testing serves a dual purpose. First, it keeps the audience alert. Second, it indicates the efficiency of the presentation and the total program. These do not necessarily involve written answers. In fact, skits, and hypothetical situations tend to enliven the session. Audience participation will give the same results. An audience enjoys giving consequences or solutions to situations.

LESSON 3

PRACTICE EXERCISE

REQUIREMENT. The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. You are deciding on the use of graphic media aids in your security education program. Which of the following is considered brief, imparting their message at a glance?

A. Placards.
B. Posters.
C. TEC lessons.
D. Leaflets.

2. Who is responsible for planning the program of instruction?

A. Company commander.
B. Security manager.
C. Provost marshal.
D. Battalion commander.

3. You are considering scheduling and testing in your education program; frequent short periods of instruction are more effective than less frequent long periods.

A. True.
B. False.

4. What is the minimum requirement for orientation as prescribed by AR 381-12? (This covers Subversion and Espionage Against the U.S. Army and Deliberate Security Violation.)

A. Quarterly and initial.
B. Semiannually.
C. Initial and annual basis.
D. Bimonthly.

5. Your unit's crime prevention program and security education program have little to do with one another. They should be established separately.

A. True.
B. False.

6. Guidance on leading a crime prevention program can be located where?

A. FM 19-10.
B. FM/AR 190-20.
C. FM 119-20.
D. AR 119-20.

7. Security awareness programs are targeted toward what?

A. Persons working with classified material.
B. Key military and civilian personnel only.
C. Physical security personnel.
D. All persons employed on the installation.

LESSON 3

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	B.	Posters. Posters are good... (page 3-3, para 6a)
2.	B.	Security manager. The security manager... (page 3-4, para 9a)
3.	A.	True. Frequent, short periods... (page 3-5, para 10a)
4.	C.	Initial and annual basis... Further orientation should... (page 3-3, para 7c, d)
5.	B.	False. Security education... (page 3-4, para 8a)
6.	A.	FM 19-10. FM 19-10... (page 3-4, para 8b)
7.	D.	All persons employed on the installation. All personnel are... (page 3-3, para 7b)

LESSON 4

SUPERVISE PHYSICAL SECURITY FORCE OPERATIONS

Critical Task: 191-386-0016

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to plan and supervise a security force operation.

TERMINAL LEARNING OBJECTIVE:

ACTION: Plan and supervise a security force operation.

CONDITION: You will have this subcourse, paper and pencil.

STANDARD: To demonstrate competency of this task, you must achieve a minimum score of 70 percent on the subcourse examination.

REFERENCES: The material contained in this lesson was derived from the following publication: FM 3-19.30.

INTRODUCTION

The security force consists of special persons. They are organized, trained, and equipped. Their purpose is to provide physical security for the command. This force is the one through which protection from threats to a post is planned and begun. Normally, the security force consists of military or civilian personnel. It may consist of a combination of both. In the field of law enforcement and investigations jurisdiction is determined by the provost marshal or security officer. It is based on location and ownership of the post. Jurisdiction is also based on federal and state law.

PART A - Security Force Mission and Function

1. General. Security forces protect personnel, property, and operations on post. They do so through a combination of the following missions and functions. These duties are performed in accordance with the physical security program and procedures. Protection is also carried out per the authorities on the post.

a. They must enforce the personnel identification and movement control systems.

b. Observation and patrolling perimeters, areas, structures, and activities of security interest are part of their duties. In-depth security against enemy or terrorist acts may be accomplished by patrol. Security is also possible by observation outside the perimeter of the post.

c. Forces must apprehend persons attempting to gain unauthorized access.

d. They must check sensitive areas during nonoperational hours.

e. Forces must perform essential escorts.

f. They must respond to protective alarms.

g. They must perform security duties, as required. In the event of fire and other disasters or disorders, however, security forces should not be dedicated to fire fighting duties since fires may be deliberately started as a diversion.

h. Security forces must otherwise safeguard personnel, property, and information. They must protect these from unauthorized access, loss, theft, or damage. This may include duties outside the post. Examples might be port and harbor operations and road security.

2. Types of Security Forces.

a. Military. This type consists of MPs and/or other military persons assigned to the post. Normally, MPs perform the security duties which require special training and experience. The interior guard type of security is performed by regular unit troops. MPs are also used in a supervisor or combined role with civil service guards.

b. Civil Service. Civil service security personnel are uniformed. They are civilian employees of the government. They are trained and organized along semimilitary lines. The organization may be completely civil service employees under military supervision. In either case, it is under the operational control of the provost marshal or security officer.

c. Labor Service Personnel. Labor service units are composed of local civilians. They are organized and used in a theater of operations. These units were organized after World War II. Since that time they have had very good records in the physical security field. These guards are of many nationalities. They are specially uniformed, organized, and equipped.

d. Auxiliary Force. Auxiliary security forces function to supplement the regular force. They also relieve the regular force of additional duties. This may occur during a disaster or national emergency. Auxiliary forces should be drawn from personnel on post. Retired persons may be used if they are physically capable. The auxiliary security force should be organized in the same way as the regular security force: Certain regular security force personnel should be trained in supervisory positions in preparation to lead the auxiliary force in case the need arises. Auxiliary forces should be

trained. They should also be equipped to function effectively. A uniform, or at least a distinctive armband should be provided. Arms and other guard equipment can be issued, as needed. These would come from regular security force supply channels.

e. Contract Security Guard. Contract security guard service is sometimes procured from commercial firms. These would be those firms particularly specializing in security-type duties. These services have also been used in overseas commands.

3. Security Force Qualifications. Security persons should possess the following traits:

a. Alertness.

b. Judgement.

c. Confidence.

d. Physical fitness.

e. Tact.

f. Self-control.

4. Planning Manpower Requirements. Manpower requirements to protect and guard a post must be determined. Therefore, a detailed analysis of the post and its mission is necessary to identify several facts. It must first be known when control and protective services are required. Second, it must be determined what type of service is needed at each location. Third, the number of men required for the type of service required at each location must be decided. Fourth, the time during which the service is required at each location should be known. Fifth, the amount of supervisory and administrative overhead needed to support the service must be known. Sixth, additional allowances needed to compensate for leave, sickness, and other contingencies must be determined. Seldom will any installation have enough manpower to provide all the desired security force personnel. As physical security officer, you would carefully program your resources. You must focus on the economical and efficient use of the manpower resources available and required. The following must be kept in mind during all planning for manpower.

a. Threats to security -human or natural.

b. Perimeter extremities.

c. Vulnerability and criticality of the activity - the accessibility and effect of partial or complete loss.

d. Location of the activity.

e. Security classification of the activity.

f. Security force's 24-hour operation.

g. Vehicles, equipment, weapons, and communications.

5. Computation of Security Force Requirements.

a. The degree of security achieved will depend upon the efficiency of its security force. However, seldom will any post have enough manpower. It can seldom provide all the people desired. It is very important, then, that the most economical and efficient use be made of the force. This can be done only by well-planned, accurate programming. Annual man-hour commitments must be carefully computed. Also, individual performance must be determined. These two acts must occur before reliable manpower needs can be forecast.

b. Annual commitments for posts and patrols are expressed in terms of man-hours per year. To operate a post or patrol which is active the same number of hours each day, man-hours per year required must be obtained. This figure is found by first multiplying the number of men required times the number of hours the post is operated per day. Next, multiply that figure by the number of days per week. Then multiply that answer by the number of weeks per year. Man-hours per year equals the number of men; that is multiplied by the hours per day; that figure is multiplied by days per week; the last figure is multiplied by weeks per year. Computation examples are listed below.

Example #1: Post #1 requires 2 men, is operated 24 hours per day, 7 days each week.

Man-hours per year -2 (men) x 24 (hours per day) x 7 (days per week) x 52 (weeks per year) = 17,472

Example #2: Post #2 requires 1 man, 16 hours per day, 5 days each week.

Man-hours per year -1 x 16 x 5 x 52 = 4,160

c. Some posts or patrols may be required only on normal operational days. Others may be required at all times when the installation is non-operational. Post #5 requires 1 man, 1600-0800, Monday through Friday, and 24 hours on Saturday and Sunday. Man-hours per year:

Monday through Friday = 1 x 16 x 5 x 52 = 4,160
Saturday and Sunday = 1 x 24 x 2 x 52 = 2,496

Total 6,656 man-hours per year

6. Individual Security Force Performance.

a. The amount of work which can be expected from each person may vary. The difference may be due to the person used or to the geographical location. It may be due to climatic conditions and military situation. Figures listed

below are based on military and civil service security forces. These are persons employed in the U.S. under peacetime conditions.

b. Civil service employees.

(1) The basic work week for civil service employees is 40 hours. If an individual works 52 weeks, this would total 2,080 man-hours per year. However, he will not be available for the full five days of each week in the year. Therefore, for planning purposes, it must be assumed that he will be absent as follows:

(a) Twenty days annual leave authorized for each employee with 3 to 15 years service (this is accepted as average for most forces).

(b) Ten national holidays or compensatory time authorized for each employee.

(c) Thirteen days sick leave authorized for each employee. (Each person will not take the full amount; some may have serious illnesses which will cause them to be absent longer.)

(d) Active duty training for reserve military personnel, attendance at schools, and other administrative absences may result in a further reduction in productive hours. However, these absences cannot be programmed accurately. Therefore, no allowance is made in the overall computation.

(2) Total anticipated absences for each civil service employee as indicated above will be 43 days or 344 hours each year. Subtracting this amount from 2,080 leaves 1,736 man-hours each year. This is the amount of productive work which can be expected from each employee.

c. Military personnel.

(1) The basic work week for military personnel is 44 hours. Of this, a minimum of 4 hours should be allocated for other duties. Examples are mandatory training, inspections, and care and cleaning of equipment. This leaves 40 hours per week for productive work. Each soldier should be present 52 weeks per year. If so, he should be able to produce 2,080 man-hours of productive time.

(2) As with civil service employees, military personnel will not be available at times. This is due to ordinary leave, sickness, or schools. It can also be due to shortages in assigned personnel and other administrative reasons. To compensate for this, a manpower increase is sometimes allowed. An 11 percent increase in manpower is authorized for posts or activities operated on a continuous basis. This means that 1.11 men will be required to perform 2,080 man-hours of productive time. Divide 2,080 by 1.11. You will find that one soldier may be expected to perform 1,874 man-hours per year. It should be noted that this is slightly more than can be expected from civil service personnel.

7. Manpower Requirements. First, the total post and patrol commitments and the pertinent individual performance factor should be determined. After that is done, the manpower requirements can be computed. Determine the total number of security men required. Find this number by dividing post and patrol commitments by individual guard performance, e.g.:

$$\text{Guards required} = \frac{\text{Post and patrol commitments}}{\text{Individual performance}}$$

a. You may need to compute manpower requirements for a civil service security force. If so, the figure of 1,736 man-hours (the actual productive time) is put into the formula for individual guard performance, i.e.:

$$\text{Civil service personnel required} = \frac{\text{Post and patrol commitments}}{1{,}736}$$

Using the above formula, you can determine civil service manpower requirements for various commitments, e.g.:

Assume that post and patrol commitments total 91,120 man-hours per year. Manpower requirements, then, are calculated civil service personnel required = $\frac{91{,}120}{1{,}736}$ = 52.48 or 53 employees.

b. If military personnel are to be used, then the figure 1,874 (the actual productive time) is substituted into the basic formula, e.g.:

$$\text{Military personnel required} = \frac{\text{Post and patrol commitments}}{1{,}874}$$

Using this formula, you can find military manpower requirements for various commitments, e.g.:

$$\text{Military personnel required} = \frac{91{,}120}{1{,}874} = 48.62 \text{ or } 49 \text{ soldiers}$$

c. Physical security planners must remember that these figures are valid for planning purposes only. Each security force presents a separate problem. The requirements must be calculated to fit the post.

8. Organizing Security Forces. Always take into consideration circumstances and available manpower. Doing this, security forces are organized into fixed posts, patrols, or reserves. Forces may be organized into any combination of the three.

a. Fixed posts are required at locations where the security interest is extremely critical. These are areas where mere access by unauthorized personnel is a breach of security. At these sites, material or services are critical. They are so vulnerable that loss or damage may occur if left unguarded even for short periods. At these sites also security functions

require continuous observation and action. Functions may require the continuous presence of security personnel for long periods.

b. Patrols (motor or foot) are required in certain areas. Such areas are those where two or more security interests are separated by time and space. Yet each requires periodic inspection by security personnel. Patrols may be needed where one or more stationary posts require reinforcement. When control of movement of persons and property within the area is required, patrols are needed. Also, where selective enforcement of law and order or traffic control is needed at two or more sites, patrols are required.

9. Instructions to the Security Force.

a. Communicating instructions to the security force should be in writing. There are three forms used: general, special, or temporary orders. Instruction should be clearly worded. Misinterpretation of assignments is then avoided. Review instructions at least monthly to maintain current information. Security force orders will be maintained at the post or patrol. By so doing, members can refer to them during duty hours. These orders should not be posted on unit bulletin boards.

(1) General orders are those which concern the security force as a whole. These orders are applicable at all posts and patrols. Items that must be covered include:

(a) Wearing of the uniform.

(b) Reporting for duty.

(c) Report writing.

(2) Special Orders pertain to the conduct of a permanent post or patrol. Each should have special orders issued concerning the location; duties; hours manned; arms, ammunition, and other equipment required; and instructions on the use of force in enforcement and apprehension activities.

(3) Temporary Orders are issued for a short period. They cover a special or temporary situation. These orders have no permanency at the time issued. If it can be predetermined, such orders should indicate the period of time they are valid.

b. A security force manual or handbook should be prepared containing policies, organization, operating procedures, and information. This should be given to all security force personnel as required reading.

10. Uniform and Standards of Appearance. Security force personnel should wear a distinctive uniform or uniform items which readily identifies them. Complete uniform requirements will be prescribed in current SOPs or directives. Flashlights, police whistles, notebooks, and other equipment should be included.

11. Procedures for Handling of Weapons and Ammunition.

a. Weapons and ammunition supplies must be kept in secured storage containers. This will prevent unauthorized access. AR 190-11 prescribes procedures for storage of weapons when not in use. Weapons and ammunition must be issued only under proper supervision for authorized purposes. They must be accounted for by individual members. Accounting must occur right after completion of the period or purpose for which issued.

b. Weapons. The authority to carry firearms on security duty is derived from officers of field grade rank or higher, or civilian equivalent of grade General Schedule (GS) 12 or above. All members of the security force should be authorized to carry firearms while performing official duties. They are normally armed with either the revolver, .38-caliber; or they may carry a pistol, .45-caliber or 9mm. Weapons normally are loaded with live ammunition. This is the case except where banned for safety reasons. Often, weapons are required to sustain the security force in an emergency, riot, or other disturbance. These weapons should be maintained at strategic points; they should be kept in readiness for issue when needed. Privately owned weapons are not authorized while on duty.

c. Weapons inspection. Inspections should be done at the start and end of each tour of duty. Others may be scheduled to ensure proper maintenance. Others may also be needed to determine if the weapon has been fired. A written report should be prepared and filed on the discharge of any weapon. Such is the case except when firing occurred during authorized and supervised training.

12. Vehicles. Enough vehicles should be assigned to the security force as required for security patrol operations. Each vehicle should be equipped with multichannel two-way radios. There must be a primary and secondary communications system.

PART B - Security Supervisor

1. General.

a. A security supervisor must oversee and direct. His duty covers the work and behavior of others on the security force. The effective supervisor needs a complete understanding of the principles of leadership. He must know how to apply them. That way he gets maximum performance from force members.

b. The supervisor is called upon to think and act in terms of many varied jobs. He is often responsible for the selection and induction of the force. Their training, productivity, safety, morale, and advancement is also his duty. He must understand these and all other employment aspects of his force.

c. It is necessary to maintain an alert, presentable, and efficient security force. To do so, there must be constant and constructive supervision. Supervisors must be in evidence. They must also conduct themselves as models of neatness. They must employ fair play, efficiency, and

loyalty. The morale and efficiency of a force reflects directly the quality of its supervision.

d. The ratio of supervisor personnel to security guard personnel should be determined by the characteristics of each post. In small compact posts, the ratio may be higher than at very large posts. In general, there must be enough supervision to enable the inspection of each post and patrol twice per shift. Also, there must be enough backup personnel to provide for sick and annual leave. It is also a must that supervisors be in contact with guard headquarters. That way they can control emergencies that may arise. Specific duties of a supervisor include the inspection and briefing of the relief shift. This occurs prior to its going on duty. The supervisor must also inspect guard posts, vehicles, and equipment. He performs these duties during visits to the posts and patrols.

2. Supervisor's Relationship to Security Force. Supervisors should strive for the creation of loyal security force. Supervisors should work to maintain a force with high morale. Following are some ways by which this may be done.

a. Proper training and supervision.

b. Direction of the security force in an objective, businesslike manner. At the same time, supervisors should be considerate of the personal welfare of force members.

c. Application of basic principles of human relations. The effective supervisor must know that there will be individual differences among members. He should be guided by the principle that subordinates are motivated in different ways; ambition can be stirred or pride hurt by his regard, or lack of it, for their welfare and feelings. A good supervisor must understand the needs and desires of his security force; he represents them. They should be made to feel that he is the one with whom they can talk and discuss their problems on a personal basis.

d. A good supervisor will develop depth in a security force. This will assure continuity of operations.

e. A good supervisor has a nice reputation. He is honest, considerate, and willing to listen to both sides of a grievance. He must have knowledge of his job and the principles involved. He must have the ability to teach these principles to his force. All of these qualities will help greatly in building confidence among his security guards. These traits will also aid in securing cooperation of his guards. Specific techniques for securing cooperation include the following:

(1) Security guards should be made to feel their job is an important one.

(2) Security guards should be given a chance to express their thoughts, likes, and interests to the supervisor.

(3) Supervision should be based on individual needs.

(4) Supervisors should recognize achievement. For example, a "guard of the month program" may be implemented. Appropriate reward can then be given for outstanding effort or achievement.

(5) Security guards may be recommended for advancement for outstanding effort or achievement.

(6) The supervisor should maintain an air of impartiality in dealing with his subordinates.

f. An effective supervisor develops good security force discipline. He does so by setting rules which are just and complete. Such rules should be easy to administer and understandable. Sometimes a supervisor needs to take corrective action involving his security force. If so, it may only call for "setting a man straight." This is a recommended technique for supervisors to consider. Types of situations in which verbal corrective action should be considered are as follows:

(1) When deficiency is due to lack of knowledge or training.

(2) When error is trivial.

(3) When action is first offense.

(4) When due to old habits.

g. Under some circumstances the supervisor may need to take constructive disciplinary action. Occasions for this might be as follows:

(1) When verbal corrective action has failed.

(2) In cases of flagrant or willful violation of post or security rules.

(3) When loss, damage, or hazard is caused through negligence.

h. Disciplinary action should be handled calmly and privately. The supervisor should have full knowledge of the facts. Sometimes punitive action is called for. If so, the UCMJ, or pertinent civilian personnel regulations covering probation and discharge, should be consulted. It is well to remember that these are serious actions; they should be taken only when all other measures have failed. The supervisor should bear in mind the requirements for documented proof. Such proof of events and actions necessitating disciplinary action is a must. When the decision has been reached as to the propriety of probation or reprimand, further action should be pursued. This should be done vigorously and without fear of reprisal. It should also be done without seemingly excessive administrative burden.

3. Alleviating Security Force Problems.

a. Efforts should be made by physical security supervisors to maintain a good relationship with subordinates through the proper application of leadership principles.

b. The nature of security force operations poses some morale problems that do not normally confront other people. The security force is required to be effective at all times, regardless of the weather, the day, and the hour. This means duty hours on weekends, holidays, and night-hours that are usually considered to be nonduty time. This causes problems in living for both the person and his family that tend to lessen enthusiasm for the job. There is a direct relation between quality of performance and morale that forces consideration of these problems. The problem can be minimized by use of the following steps.

(1) Maintain high standards of discipline.

(2) Promote an aggressive security education program. This will ensure that each man clearly understands the importance of his job. Each man must understand the consequences of any breach of protective barriers. Each man should see that the human element in security operations makes the difference between success and failure.

(3) Arrange shifts so that personnel will periodically have a 48-hour period free from duties.

(4) Consider shift rotation as one solution to security force boredom. The transfer of a person from one shift to another could be considered a reward. This is due to the working hours of some shifts being less desirable than others. For better security service, the integrity of the shift should be maintained as a unit.

(5) Establish good recreational facilities at or near security force sites. Start an organized athletic program, also. This will help develop loyalty, pride, and enthusiasm for the unit or post.

(6) When practical, hot food should be given to those going on post and those coming off. This is a definite morale factor.

c. Sometimes both military and civilian personnel are used at a post or activity. If so, the provost marshal or physical security officer should ensure equal treatment for security force members. Any instructions or corrective action should be put out to the force by the appropriate supervisor.

PART C - Training

1. General.

a. Basic Training (preservice).

(1) MP personnel assigned to physical security will have at least completed basic and advanced training.

(2) A continuing program will be started to promote the education and motivation of security personnel. The continuous proficiency of these personnel must be maintained. To do so, commanders will start a security training program. It should be job related and include the following:

(a) Normal security functions of personnel identification; movement procedures and escort functions; operation and use of intrusion detection and alarm systems; operation and use of security communications equipment and systems security vehicle operation; and appropriate record keeping.

(b) Legal authority, responsibility, and jurisdiction of sentries on duty. This includes search and seizure and the use of deadly force.

(c) Duties in the event of alert, natural disaster, or emergency.

(d) The type and location of hazardous and vulnerable equipment and material.

(e) The location of fire protection equipment; the location of utility switches and first aid facilities.

(f) The location of primary and alternate communications systems.

(g) Training for supervisory personnel. To include availability and evaluation. Also to include the use of intelligence and counterintelligence services.

(h) Briefings on security incidents, current and potential threats. Briefings on intelligence and counterintelligence procedures and capabilities. Also, briefings on security force reaction to intruders. In addition, practical exercises in defense techniques to counter these threats.

(i) Common forms of sabotage and espionage activity.

(3) Security personnel will be thoroughly familiar with their weapon(s). Familiarization will include proper care and maintenance. It will also include safety features and range firing within the previous 12 months.

(4) Each person shall have specialized training regarding his specific duties and duty location. This training is in addition to training prior to security assignment.

b. In-service training. When a new security guard is assigned, he must be taught about conditions peculiar to his post. When possible, his first

assignment should be with an experienced security guard. A continuous requirement will be additional in-service training. Also, periodic retraining of personnel is necessary. This will be done to review basic material and other subjects applicable to the specific post.

c. Assess performance of security forces.

(1) Evaluation of training.

(a) Tests or examinations (FM 21-6) for evaluating security guard performance are necessary. Such testing is also necessary for an effective training program. These tests, whether oral, written, or a type of performance test, should be given at least once a year. By so doing, supervisors can determine whether high standards of proficiency are being achieved and maintained. A testing program will also aid in improving security training by:

1 Discovering gaps in security training.

2 Stressing main points.

3 Evaluating teaching methods.

(b) Training received by security at their units should be entered in unit training charts or records. This record will help to:

1 Indicate individual degrees of skill.

2 Set priorities of instruction.

3 Present a complete picture of the guard force training status.

2. Vulnerability Tests.

a. Many security demands are routine, of a repetitive nature, and involve much solitude. Because of this, personnel must make special efforts; they must overcome a tendency to relax in doing their duties. To check on this weakness, certain tests may be used. They will help keep personnel aware of their responsibilities. The tests will also serve to point out other weaknesses in the security system. These are vulnerability tests. They are normally designed by the provost marshal or the physical security manager. The tests consist of attempts to breach security in one way or other. An example would be entering or attempting to enter a restricted area through deception. The types of deception which may be used are almost unlimited.

b. Test objectives.

(1) A vulnerability test gives the CO an estimate of the vulnerability of his post or facility. It tests the effectiveness of the security force and other personnel; it alerts personnel to the techniques that

could be used by an intruder; and it provides material for corrective instruction.

(2) Specifically, the test should examine:

(a) Improper enforcement of identification and control procedures by security personnel. Examples are failure to:

1 Determine authority for entry.

2 Scrutinize identification media. The ways of using fake credentials to dupe security are many. There is only one way to detect such trickery; that is, know the details of each type of access credentials; examine them thoroughly. Security tests and inspections have shown that unauthorized persons have been granted access to restricted areas. They have gained access by altering or forging passes. They have faked identification by telephone. They have also gained access by playing upon the sympathy of security personnel with excuses.

3 Ascertain identity.

4 Detain unauthorized persons.

5 Conduct immediate preliminary search of suspects.

6 Enforce security procedures.

7 Report security violations.

(b) Susceptibility or gullibility of security personnel. Personnel often believe plausible stories by intruders. Sometimes these stories come from members of the security force and other post personnel. This inclination to believe a person who may be trying to gain illegal access to a restricted area is the product of two factors. These factors are monotony and a desire to save time. Persons authorized into a restricted area are often busy coming and going; therefore, it is easy for them to deceive the security personnel with slight evidence. Verifying hundreds of valid access credentials is boring. This can dull the sensitivity to detect one which is false. Many attempts to dupe security personnel involve false credentials. They also involve assumed rank or falsely marked vehicles.

(c) Unauthorized disclosure of information by security and other personnel of the post.

c. Test planning and preparation. Detailed planning and preparation is a requirement for effective testing of security. Planning should include the following:

(1) Plan in secrecy to avoid alerting post personnel. Prior knowledge by the security forces or others produces invalid test results. It thus defeats the purpose of the test.

(2) Set a priority of targets that seem more vulnerable than others. Do not test the same target on a continuous basis. Try to test all eligible targets over time. This will keep all personnel alert, rather than those of only one area.

(3) Select qualified people to conduct vulnerability tests. Criteria for personnel should include the following:

(a) All personnel should have appropriate security clearances. These should be at the same or higher level of the area or post to be entered. Such clearances preclude any compromise of security interests if a safe is found open. Also, if an area with classified matter is entered, security will not be compromised.

(b) Members of the test team should be unknown to members of the security force. Members should also be unknown to other personnel of the post or area.

(c) Team members should be capable of quick thinking to adapt to their cover stories.

(d) Members should be able to bluff in a convincing manner.

(e) The cover story should originate with the provost marshal or physical security manager. A well-contrived cover story is necessary. It should sound convincing to provide a good test of the security force.

(4) Obtain appropriate material for testing. This may include:

(a) Clothing appropriate to assumed identity.

(b) Props necessary to support cover story.

(c) Tools appropriate to assumed identity, such as repairman or plumber.

(d) Transportation.

(e) False or altered credentials.

(f) Simulated sabotage devices to provide realism. These might include explosives, incendiaries, abrasives, corrosive acids, etc. These devices should meet the following criteria:

1 The device should be suitable for the target.

2 The device should be the same size and weight as the genuine article.

3 The device should be properly labeled like the one it is simulating.

4 For realism, simulated time of detonation should be indicated on the device. There is always the chance that the device will be found before the simulated time of detonation.

5 Planting of the device should be related to the type used. It should be placed to simulate the greatest amount of destruction or to achieve the desired results.

d. Test instructions.

(1) The officer in charge of the test should select the method or techniques to be used. Selection should be based on the ability of testing personnel. It should also be based on supporting materials available.

(2) This officer should provide for flexibility in selection of targets. His orientation to team members should include the following instruction:

(a) Exploit any security weakness that becomes evident during the test.

(b) Change tactics to take evasive action as necessary.

(c) Strike targets of opportunity.

(3) Remember the test objectives.

(a) Estimate vulnerability for the CO.

(b) Determine effectiveness of security force and other personnel.

(c) Alert guard force and CO to possible techniques of an attempted security breach.

(d) Provide information for corrective action.

(4) Personnel assigned to conduct vulnerability tests should be given only limited information about the post or facility. Such knowledge would be the same that an outsider would normally have or could get reasonably.

e. Test safety. Instructions to test team members should also include safety precautions. Test personnel should not:

(1) Scale barriers of any kind. Guards may have instructions to fire.

(2) Forcibly resist apprehension. There is too much danger involved. By resisting apprehension, personnel will nullify benefits to be achieved.

(3) Use dangerous materials. These might cause harm to any person involved directly or indirectly.

(4) Use any action that might influence normal operations, safety, or equipment of the post.

f. Techniques for infiltration of security areas. Personnel leading vulnerability tests should consider the following techniques. These are to be used for infiltration of secured areas.

(1) Enter through unguarded gates or open areas. These should not be under observation by security forces or other persons.

(2) Use false or altered passes or badges. Show these at active gates manned by security. They usually give only a slight glance at these IDs.

(3) Enter through areas without showing identification.

(a) One way is to bypass security forces. Do this by mingling with a work group entering the area.

(b) Another method is to get permission to enter the area. Claim loss of identification; use a plausible story.

(c) A third way involves deception by false representation. Here a member of the test team poses as a high-ranking officer or civilian dignitary. Or he might pose as a repairman, installer of equipment, inspector, etc. These are people who have legitimate business in the area.

g. Neutralization of escorts. Making successful entrance to a security area is only the first step. Testers must then, in many cases, neutralize an assigned escort. They must do so to accomplish the test mission. Procedures for neutralization include the following:

(1) When operating as a team, use ruses to divert the escort's attention.

(2) Request use of latrine; leave if not accompanied by escort.

(3) Devise any other means as opportunities occur. However, use no force to overpower the escort.

h. Planting simulated sabotage devices. Procedures to follow for planting simulated devices include the following:

(1) The device should be planted appropriately, if access can be gained. It should be put in the place where it would do the most damage.

(2) Place on any vehicle entering the area.

(3) The device can be given to authorized personnel entering the area. Do so by using bribery or coercion. This could also be done by secreting it in their clothing or accessories such as purses or briefcase.

i. Upon completion of vulnerability tests, results should be reported. This should be done preferably in writing. The report should be carefully reviewed and analyzed by the provost marshal, physical security manager, and those with a need to know. The review and analysis should provide an evaluation of the physical security program. The report should also serve as a basis or guide for effecting necessary changes. Review and analysis of methods and procedures used for vulnerability tests give guidance for future tests.

LESSON 4

PRACTICE EXERCISE

REQUIREMENT. The following questions are multiple choice. You are to select the one that is correct. Indicate your choice by CIRCLING the letter beside the correct choice directly on the page. This is a self-graded lesson exercise. Do not look up the correct answer from the lesson solution sheet until you have finished. To do so will endanger your ability to learn this material. Also, your final examination score will tend to be lower than if you had not followed this recommendation.

1. You are computing manhours required for posts/patrols. You must remember that, in terms of total manhours available, which of the following applies?

A. Military and civilian guards are the same.
B. More hours are available for civilian guards.
C. More hours are available for military guards.
D. Manhours are not important when computing patrol requirements.

2. To be an effective security guard supervisor, you must always keep in mind which of the following?

A. Sometimes, guards must work 7 days each week.
B. The nature of security force operations poses some morale problems. These are problems that do not normally confront other personnel.
C. Because of age, civilian guards need more sick leave time.
D. You must visit each post four times per shift, when possible.

SPECIAL SITUATION: A change in mission of the post has necessitated more security measures. Those measures will increase your civil service security force requirement as follows: (Posts #4 and #5)

Post #4 (one man) to be manned only during working hours. Normal working hours for the installation are from 0800-1600, Monday through Friday. No overtime will be programmed.

Post #5 (one man) will be manned only during nonworking hours.

3. Assume that no other manpower requirements are to be considered. The number of added security personnel which should be hired to man posts #4 and #5 are how many?

A. 5.0.
B. 6.0.
C. 3.0.
D. 4.0.

4. For planning purposes you should expect each civilian person to work each year, a total of how many hours?

A. 1,866 hours.
B. 1,792 hours.
C. 1,816 hours.
D. 1,736 hours.

5. Which statement concerning the communications system in a security force vehicle is CORRECT?

A. Have multichannel capabilities.
B. Have a primary and secondary system.
C. Have power source for fixed posts only.
D. Responses a and b.

6. Which of the following statements refer to the results of any vulnerability test of the security force?

A. They should be limited to the provost marshal, physical security manager, and those who have a need to know.
B. Be written up in a weekly post paper. That way everybody will know that your security force is doing their job.
C. Be verbally briefed so there is no written record.
D. Be carefully reviewed by the post CO so he can fire anyone that makes a mistake.

7. Which subject in a proposed basic training course for the security forces should be DELETED?

A. Weapons safety and qualification.
B. Disarming and removal of explosives.
C. Authority of the individual.
D. Employee and public relations.

8. Which statement about the weapons of your civilian security force is CORRECT?

A. They should be issued by the post and kept there except in the course of official duty.
B. The weapons may be privately owned if properly controlled.
C. Authorization cards to carry the weapons are not necessary.
D. Under no circumstances can a guard carry the weapon off post.

9. The security force may be organized by which of the following?

A. Fixed post deployment.
B. Patrol deployment.
C. Reserves.
D. All three or any combination of the above.

10. Vulnerability tests require detailed planning by the person in charge. Proper planning should include provision for which of the following?

A. Incapacitating the security guards through the use of non-deadly weapons.
B. Assuming that the security guards know a test is being conducted. That way injury to personnel will be avoided.
C. Use of actual sabotage devices so that realism will be achieved.
D. Assuring that test personnel have a security clearance as high as the area they are trying to enter.

LESSON 4

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

Item		Correct Answer and Feedback
1.	C.	More hours are available for military guards. It should be noted... (page 4-5, para 6c(2))
2.	B.	The nature of security force operations... The nature of security... (page 4-11, para 3b)
3.	B.	6.0 You may need to... (page 4-6, para 7a)
4.	D.	1736 Subtracting this... (page 4-5, para 6b(2))
5.	D.	Responses a and b. Each vehicle should... (page 4-8, para 12)
6.	A.	They should be limited to the provost marshal, physical... The report should be... (page 4-18, para 2i)
7.	B.	Disarming and removal of explosives. A continuing program... (page 4-12, para la(3))
8.	A.	They should be issued by the post and kept there... Weapons and ammunition... (page 4-8, para 11a)
9.	D.	All three or any combination of the above. Doing this, security... (page 4-6, para 8)
10.	D.	Assuring that test personnel have a security... All personnel should... (page 4-15, para 2c(3)(a))